50

Notice of Allowability	Application No.	Applicant(s)	
	10/039,595	GLEW ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *19 April 2007*.

2. ☒ The allowed claim(s) is/are *21-40*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 29 June 2007
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. Claims 1-20 have been cancelled.

2. Claims 21-40 have been added.

3. Claims 21-40 are pending.

Information Disclosure Statement

4. The Information Disclosure Statement respectfully submitted on 29 June 2007 has been considered by the Examiner.

Response to Arguments

5. Applicant's arguments filed 19 April 2007 have been fully considered and they are persuasive.

Allowable Subject Matter

6. **Claims 21-40** are allowed.

7. The following is an examiner's statement of reasons for allowance: The present invention is directed towards an authenticated code module comprising a value that attests to the authenticity of the module. The value is encrypted with a key corresponding to a key of a computing device that is to execute the module. Claims 21 and 27 identifies the uniquely distinct features "**accessing a key embedded in the computing device in one of a processor, a chipset or a physical token and authenticating the code module in the private memory using the embedded key**". Claim 33 identifies the uniquely distinct features "**a private memory and a processor coupled with the private memory to load a code module into the private memory**

and to authenticate the code module using a key embedded in one of the processor, a chipset and a physical token".

The closest prior art, Davis et al. (US Patent No. 6,401,208) discloses a cryptographic device is implemented in communication with a host processor to prevent the host processor from performing a standard boot-up procedure until a basic input output system (BIOS) code is authenticated. This is accomplished by a cryptographic device which is addressed by the host processor during execution of a first instruction following a power-up reset. The cryptographic device includes a first integrated circuit (IC) device and a second IC device. The first IC device includes a memory to contain firmware and a root certification key. The second IC device includes logic circuitry to execute a software code to authenticate the BIOS code before permitting execution of the BIOS code by the host processor. However, either singularly or in combination, Davis et al. fail to anticipate or render the claimed limitation wherein accessing a key embedded in the computing device in one of a processor, a chipset or a physical token and authenticating the code module in the private memory using the embedded key and a private memory and a processor coupled with the private memory to load a code module into the private memory and to authenticate the code module using a key embedded in one of the processor, a chipset and a physical token.

The closest prior art, Potkonjak (US Patent No. 7,017,043) discloses the present invention is related to systems and methods for adding a signature to circuit design. In one embodiment, a first set of constraints used to specify a functional portion of the circuit design is received. A second set of constraints used to specify the signature is

received as well. The circuit design is generated based on at least the first constraints and the second constraints, wherein the signature is embedded in the functional portion. However, either singularly or in combination, Potkonjak fail to anticipate or render the claimed limitation wherein accessing a key embedded in the computing device in one of a processor, a chipset or a physical token and authenticating the code module in the private memory using the embedded key and a private memory and a processor coupled with the private memory to load a code module into the private memory and to authenticate the code module using a key embedded in one of the processor, a chipset and a physical token.

The closest prior art, Wong (Pub No. 2002/0150252) discloses a way of protecting the configuration bits of the user of a configurable integrated circuit is described. The user-configurable integrated circuit has a decryption circuit block which decrypts configuration bits which have been encrypted by a plurality of encryption keys corresponding to a plurality of corresponding decryption keys for programming the integrated circuit into a desired configuration. The decryption circuit block receives the plurality of decryption keys from a corresponding plurality of decryption key circuits, at least one of which is embedded in the integrated circuit so as to prevent accessibility of the decryption key. Other decryption key circuits may be part of the integrated circuit or off-chip for accessibility of their decryption keys for ready identification of their owners; still other decryption key circuits may be embedded in the integrated circuit for inaccessibility. Such an arrangement permits the protection of the user's configuration from competitors and of the providers' IP from unauthorized usage by the user of the

integrated circuit. However, either singularly or in combination, Wong fail to anticipate or render the claimed limitation wherein accessing a key embedded in the computing device in one of a processor, a chipset or a physical token and authenticating the code module in the private memory using the embedded key and a private memory and a processor coupled with the private memory to load a code module into the private memory and to authenticate the code module using a key embedded in one of the processor, a chipset and a physical token.

8. Therefore, **claims 21,27, and 33** and the respective **dependent claims 22-26,28-32 and 34-40** are in condition for allowance.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/cdf/
cdf
July 23, 2007

/Matthew B. Smithers/
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137